ROSSBACH LAW, P.C.
William A. Rossbach
401 North Washington Street
P.O. Box 8988
Missoula, MT 59807-8988
Phone: (406) 543-5156
Email: bill@rossbachlaw.com

[Additional Counsel on Signature Page]

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MONTANA

BUTTE DIVISION

RICHARD OLIVIERI and LAUREN WOON, on behalf of themselves and all others similarly situated, Plaintiffs, v. AT&T, INC., AT&T MOBILITY LLC, SNOWFLAKE, INC., Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Richard Olivieri and Lauen Woon ("**Plaintiffs**") individually and on behalf of all others similarly situated, brings this Class Action Complaint (the "**Complaint**"), and alleges the following against Defendants AT&T, Inc. and AT&T Mobility LLC (collectively, "**AT&T**") and Snowflake, Inc. ("**Snowflake**") (together, "Defendants"), based upon personal knowledge with respect to themselves and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. AT&T, Inc. is the world's third-largest telecommunications company by revenue and the second-largest wireless carrier in the United States.

2. On July 12, 2024, AT&T announced that records of calls and texts of "nearly all" its wireless customers and customers of mobile virtual network operators ("MVNO") had been illegally downloaded from its workspace on a third-party cloud platform between April 14 and April 25, 2024, in a massive security breach ("Data Breach").

3. The stolen data contains phone numbers of both cellular and landline customers of around 110 million AT&T customers, as well as AT&T records of calls and text messages — such as who contacted who by phone or text — during a six-month period between May 1, 2022 and October 31, 2022. Some of the stolen data

also includes customer records from January 2, 2023.

4. According to AT&T the stolen data "does not contain the content of calls or texts," but does include calling and texting records that an AT&T phone number interacted with during the six-month period, as well as the total count of a customer's calls and texts, and call durations – aka metadata. Some of the stolen records include cell site identification numbers associated with phone calls and text messages, information that can be used to determine the approximate location of where a call was made or text message sent.

5. The nature of the compromised information is uniquely sensitive. For example, as noted by CNN, cybercriminals can now identify relationships among phone numbers, a useful data point for hackers to make scams more believable. As just one example, hackers can now see what banks customers are in regular contact with and send a more effective phishing attempt posing as that bank or as some other regular contact of the impacted customers.[1]

6. Wired also wrote about the "sweeping danger" of this breach, speaking with a cybersecurity expert who noted the data compromised is a "gold mine." This is especially so for attackers "looking to construct compelling phishing attacks and other scams to target individuals" or even "specific communities of people." Even

[1] https://www.cnn.com/2024/07/12/business/att-customers-data-breach-protection/index.html#:~:text=AT%26T%20said%20Friday%20that%20data,were%20also%20breached%2C%20AT%26T%20said (last visited July 15, 2024)

without contents of communications, the compromised metadata has "major implications for people's privacy and security." [2]

7. Another security expert highlighted that the potential for triangulation of customers' locations from compromised cell site identification numbers "adds a physical dimension to the already extensive privacy violation and could expose individuals to highly targeted and convincing social engineering attacks, not to mention compromising [their] physical security. . . ." [3]

8. Bloomberg reported that AT&T's third-party cloud platform involved in the Data Breach was hosted by Snowflake, a leading cloud-based data storage and analytics provider. Snowflake allows companies to store and use huge datasets on its servers.

9. In June 2024, Snowflake announced a security incident affecting as many as 165 of its customers. Mandiant, a Google-owned cybersecurity firm that assisted Snowflake in its incident response efforts, tracked the unidentified threat actor under the name UNC5537, describing it as a financially motivated threat actor.

10. Mandiant explained that since April 2024 "UNC5537 [] [was] systematically compromising Snowflake customer instances using stolen customer

[2] https://www.wired.com/story/att-phone-records-breach-110-million/ (last visited July 15, 2204)
[3] https://www.darkreading.com/cyberattacks-data-breaches/att-breach-may-also-impact-millions-of-boost-cricket-h2o-customers (last visited July 15, 2024)

credentials, advertising victim data for sale on cybercrime forums, and attempting to extort many of the victims."

11. Leaked Snowflake account credentials have been the source of other publicized breaches of brand name companies such as Ticketmaster, Santander, Neiman Marcus, and more.

12. Mandiant's investigation revealed that the threat campaign was successful because "the impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password."[4] In other words, had AT&T and/or Snowflake enabled multi-factor authentication ("MFA") this Data Breach would likely have been prevented.

13. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals' personal information ("**Personal Information**"), including but not limited to phone call and text message records for "nearly all" of AT&T's 110 million cellular customers, as well as information about the location of cellular communications towers closest to an unspecified subset of subscribers.

[4] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion (last visited July 13, 2024)

14. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect the Personal Information exfiltrated. AT&T failed to implement MFA on its Snowflake account and Snowflake failed to require customers like AT&T to implement MFA to protect their data, among other things.

15. Defendants had a duty to adequately safeguard this Personal Information under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "**FTC Act**").

16. Defendants breached their duties and disregarded the rights of Plaintiffs and Class Members[5] by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard individuals' (whose information they were required to protect) Personal Information; failing to take available and necessary steps to prevent unauthorized disclosure of data; and failing to follow proper protocols, policies, and procedures regarding MFA, among others.

17. As a result of Defendants' inadequate security and breach of their duties and obligations, the Personal Information of Plaintiffs and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiffs and Class Members have suffered injuries as a direct and proximate result of

[5] "Class Members" defined *infra*, ¶ 104.

Defendants' conduct. These injuries include: (i) benefit of the bargain; (ii) diminution in value and/or lost value of Personal Information, a form of property that Defendants obtained from Plaintiffs and Class Members and for which there is a well-established national and international market; (iii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Personal Information; (iv) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (v) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiffs' and Class Members' Personal Information; (vi) the continued and certain increased risk that the Personal Information that remains in Defendants' possession is subject to further unauthorized disclosure for so long as Defendants fail to undertake proper measures to protect the Personal Information; (vii) invasion of privacy and increased risk of fraud and identity theft; and (viii) theft of their Personal Information and the resulting loss of privacy rights in that information. This action seeks to remedy these failings and their consequences. Plaintiffs and Class Members have a continuing interest in ensuring their Personal Information is and remains safe and are entitled to injunctive and other equitable relief.

18. Plaintiffs, on behalf of themselves and all other Class Members, brings claims for Negligence, Negligence Per Se, Breach of Fiduciary Duty, Unjust

Enrichment, Breach of Third-Party Beneficiary Contract, Invasion of Privacy, Breach of Contract, Breach of Implied Contract, Violation of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*., Violation of California's Consumer Legal Remedies Act ("CLRA), California Civil Code §§ 1750, *et seq*., Violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), (Fla. Stat. §§ 501.201, *et seq*.), and Declaratory Relief. To remedy these violations of law, Plaintiffs and Class Members seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendants' data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one member of the class is a citizen of a state different from Defendants.

20. The Court has general personal jurisdiction over Defendant Snowflake, Inc. because its headquarters and principal place of business is in Bozeman, Montana.

21. This Court has jurisdiction over Defendant AT&T, Inc. because AT&T, Inc. has committed acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over AT&T, Inc. would not offend traditional notions of fair play and substantial justice. AT&T, Inc. has engaged in continuous, systematic, and substantial activities within this State, including substantial marketing and sales of services and products in connection with the Data Breach within this State. Further, a substantial part of the acts and omissions giving rise to Plaintiffs' claims against AT&T, Inc. occurred in and emanated from this District.

22. This Court has personal jurisdiction over Defendant AT&T Mobility LLC because Defendant AT&T Mobility LLC maintains and operates its headquarters in this District. Defendant is authorized to conduct business in this District and is subject to general personal jurisdiction in this state. Defendant has engaged in continuous, systematic, and substantial activities within this State, including substantial marketing and sales of services and products in connection with the Data Breach within this State. Further, a substantial part of the acts and omissions giving rise to Plaintiffs' claims against AT&T Mobility LLC occurred in and emanated from this District.

23. AT&T (AT&T Mobility LLC and AT&T, Inc.) hired Montana-based company, Snowflake, and paid Snowflake a fee in this District, to store Plaintiffs

and other affected customers' information. AT&T, thus, benefitted from the opportunity to do business in the State of Montana. AT&T's relationship with Snowflake and storing the data on Snowflake's clouds resulted in the accrual of all claims herein (the data breach at issue). Thus, AT&T has consented to be subject to personal jurisdiction in Montana.

24. Furthermore, exercise of jurisdiction over all Defendants here will further promote efficiency, as the related action against Snowflake (relating to this data breach) is already pending in this District. *See Leal v. Ticketmaster et al*., 2:24-cv-00046-BMM (filed on June 14, 2024).

25. Venue is proper under 18 U.S.C § 1391 because it is the District in which Defendant Snowflake, Inc. has the most significant contacts. Venue is proper under 18 U.S.C § 1391(b)(2) because a substantial part of the acts and omissions giving rise to Plaintiffs' claims, including those against AT&T, occurred in and emanated from this District.

PARTIES

26. Plaintiff Richard Olivieri is a citizen of Florida. Plaintiff owned or has owned two AT&T cell phones and has been an AT&T customer since his Cingular Wireless accounts were converted to AT&T in or about 2008. Plaintiff was a customer of AT&T for cellular services during the entirety of 2022, as well as January 2023.

27. Plaintiff Lauren Woon is a citizen of California. Plaintiff has been an AT&T customer since at least 2007 when Cingular Wireless and AT&T merged and specifically during May to October 2022 and January 2023.

28. Defendant AT&T, Inc. is a Delaware corporation with its principal place of business in Dallas, Texas. AT&T, Inc. is an American multi-national telecommunications holding company. It is the world's third-largest telecommunications company by revenue and the second-largest wireless carrier in the United States.[6] As of 2023, AT&T was ranked 13th on the Fortune 500 rankings of the largest United States corporations, with revenues of $122.4 billion.[7]

29. Defendant AT&T Mobility LLC is a Delaware limited liability company with its principal place of business in Atlanta, Georgia. AT&T Mobility, LLC, also known as AT&T Wireless and marketed as AT&T, is an American telecommunications company. It is a wholly owned subsidiary of AT&T, Inc. and provides wireless services in the United States. AT&T Mobility is the second largest wireless carrier in the United States, with 114.5 million subscribers as of March 31, 2024.[8]

---

[6] https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2024/1Q24/T_1Q24_Trending_Schedule.pdf (last visited July 12, 2024)

[7] https://www.marketwatch.com/investing/stock/t/financials (last visited July 12, 2024)

[8] https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2024/1Q24/T_1Q_2024_8_K_%20Earnings_801.pdf (last visited July 12, 2024)

30. Defendant Snowflake is a Delaware corporation with its headquarters and principal place of business in Bozeman, Montana. Snowflake is a publicly traded corporation listed on the New York Stock Exchange with revenues totaling approximately $829 million for the three months ended on April 30, 2024.[9] Snowflake's Data Cloud platform is used globally, with 9,437 institutions trusting Snowflake to manage and store customers' data.[10]

FACTUAL ALLEGATIONS

A. AT&T Discloses Its Second Major Breach of Customer Data This Year

31. On July 12, 2024, AT&T publicly announced that data of "nearly all" its 110 million cellular customers from May 1, 2022 to October 31, 2022 and January 2, 2023 was illegally downloaded from its workspace on a third-party [Snowflake's] cloud platform.[11]

32. According to AT&T the stolen data includes calling and texting records that an AT&T phone number interacted with during the six-month period, as well as the total count of a customer's calls and texts, and call durations — information that is often referred to as metadata. It also includes other phone numbers that an AT&T

[9] https://www.bamsec.com/filing/164014724000135?cik=1640147 (last visited June 12, 2024)
[10] https://www.bamsec.com/filing/164014724000101?cik=1640147 (last visited June 28, 2024)
[11] https://www.att.com/support/article/my-account/000102979?source=EPcc000000000000U (lasted visited July 13, 2024)

wireless number interacted with during this time, including AT&T landline customers.[12]

33. AT&T states "[t]he downloaded data doesn't include the content of any calls or texts. It doesn't have the time stamps for the calls or texts. It also doesn't have any details such as Social Security numbers, dates of birth, or other personally identifiable information. [¶] While the data doesn't include customer names, there are often ways to find a name associated with a phone number using publicly available online tools."[13]

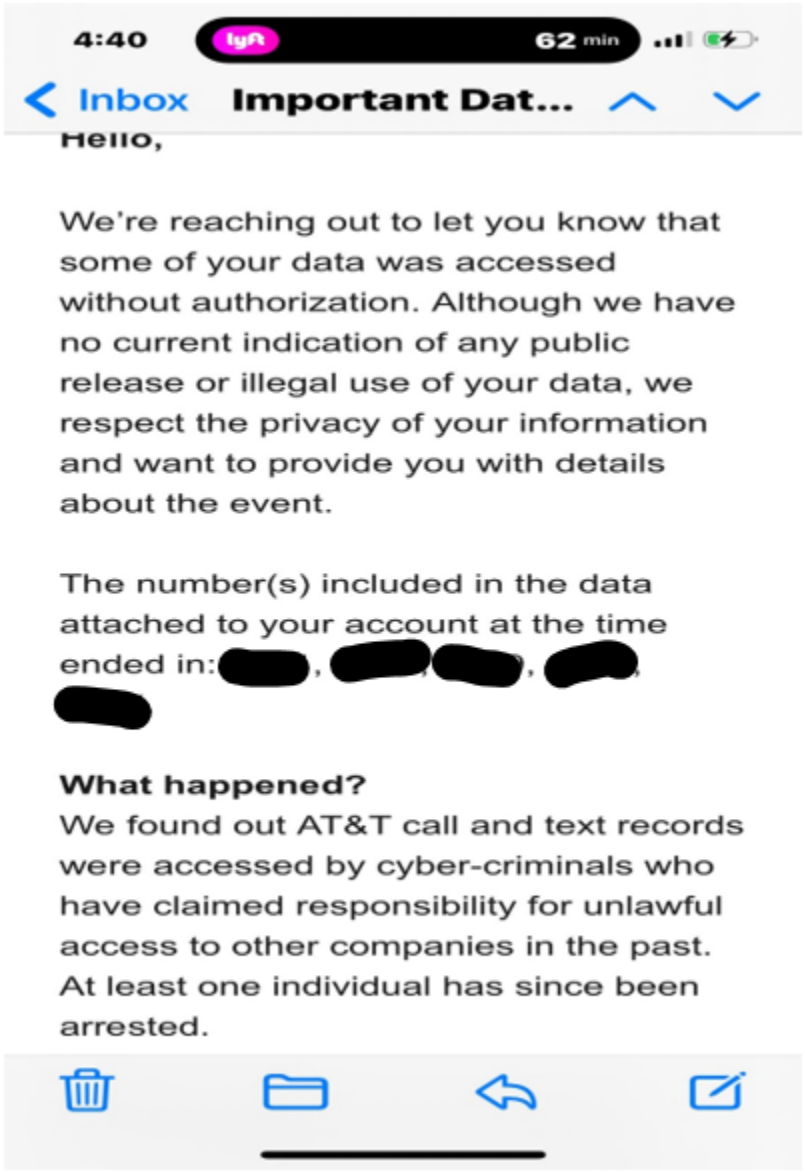
34. The Data Breach also includes a subset of records from January 2, 2023. For this subset of records, one or more cell site ID numbers associated with the phone calls and text messages were also breached.[14] This is information that can be used to determine the approximate location of where a call was made or text message was sent.

35. The stolen data also includes call records of customers with phone service from other cell carriers that rely on AT&T's network - mobile virtual network operators or MVNOs. According to public resources, those MVNOs likely include wireless service providers such as Boost Mobile, Cricket Wireless, H2O,

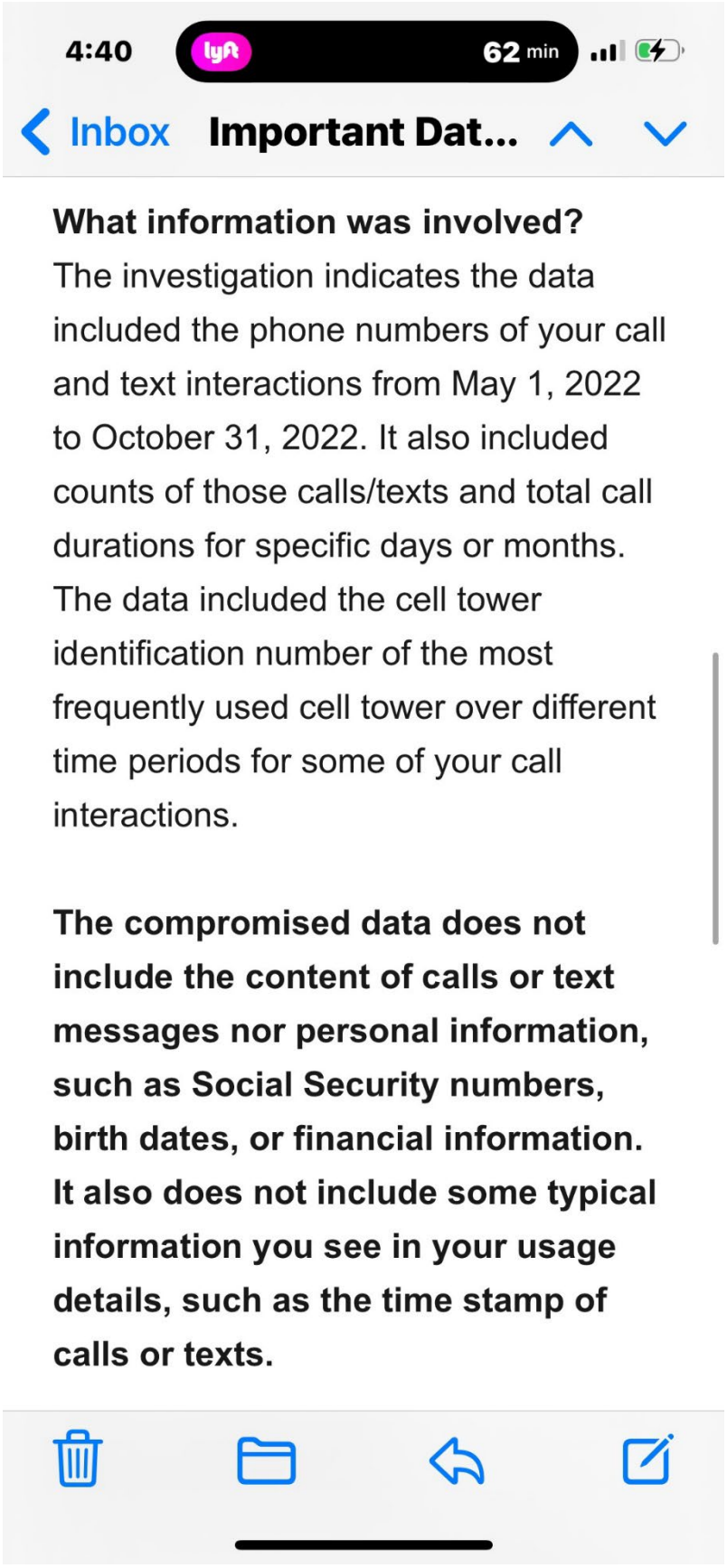
[12] *Ibid*.
[13] *Ibid*.
[14] *Ibid*.

and Straight Talk Wireless.[15]

36. On July 12, 2024, AT&T began notifying Plaintiffs and Class Members of the Data Breach via electronic mail ("Email Notice").



[15] https://www.whistleout.com/CellPhones/Guides/att-mvnos (last visited July 13, 2024)


4:40
62 min
Inbox
Important Dat...
What information was involved?
The investigation indicates the data included the phone numbers of your call and text interactions from May 1, 2022 to October 31, 2022. It also included counts of those calls/texts and total call durations for specific days or months. The data included the cell tower identification number of the most frequently used cell tower over different time periods for some of your call interactions.
The compromised data does not include the content of calls or text messages nor personal information, such as Social Security numbers, birth dates, or financial information. It also does not include some typical information you see in your usage details, such as the time stamp of calls or texts.

37. In a July 12, 2024 SEC filing AT&T provided even more details of the Data Breach. In its Form-8K disclosing a material cybersecurity incident AT&T explained:

> On April 19, 2024, AT&T Inc. ("AT&T") learned that a threat actor claimed to have unlawfully accessed and copied AT&T call logs. [] Based on its investigation, AT&T believes that threat actors unlawfully accessed an AT&T workspace on a third-party cloud platform and, between April 14 and April 25, 2024, exfiltrated files containing AT&T records of customer call and text interactions that occurred between approximately May 1 and October 31, 2022, as well as on January 2, 2023, as described below . . .
>
> . . . . . .
>
> Current analysis indicates that the data includes, for these periods of time, records of calls and texts of nearly all of AT&T's wireless customers and customers of mobile virtual network operators ("MVNO") using AT&T's wireless network. These records identify the telephone numbers with which an AT&T or MVNO wireless number interacted during these periods, including telephone numbers of AT&T wireline customers and customers of other carriers, counts of those interactions, and aggregate call duration for a day or month. For a subset of records, one or more cell site identification number(s) are also included. While the data does not include customer names, there are often ways, using publicly available online tools, to find the name associated with a specific telephone number.
>
> . . . . . .
>
> On May 9, 2024, and again on June 5, 2024, the U.S. Department of Justice determined that, under Item 1.05(c) of Form 8-K, a delay in providing public disclosure was warranted. AT&T is now timely filing this report. AT&T is working with law enforcement in its efforts to arrest those involved in the incident. Based on information available to

> AT&T, it understands that at least one person has been apprehended. As of the date of this filing, AT&T does not believe that the data is publicly available.[16]

38. On July 12, 2024, AT&T confirmed the access point had been secured, it did not believe the data was publicly available, and at least one person had been apprehended.[17]

39. 404 Media reports that John Binns, a 24-year-old U.S. citizen who was previously arrested in Turkey in May 2024, is connected to the security events. He was also indicted in the U.S. for infiltrating T-Mobile in 2021 and selling its customer data.[18]

40. This is the second breach of AT&T customer data this year. Earlier this year data of over 70 million AT&T customers — including encrypted passcodes for accessing AT&T customer accounts — was published on a cybercrime forum. AT&T confirmed the data was authentic but does not know whether the data originated from AT&T or one of its vendors.[19] The breached data includes names,

---

[16] https://otp.tools.investis.com/clients/us/atnt2/sec/sec-show.aspx?FilingId=17677638&Cik=0000732717&Type=PDF&hasPdf=1 (last visited July 12, 2024)
[17] https://www.att.com/support/article/my-account/000102979?source=EPcc000000000000U (last visited July 12, 2024)
[18] https://www.404media.co/american-hacker-in-turkey-linked-to-massive-at-t-breach/ (last visited July 13, 2024)
[19] https://www.darkreading.com/remote-workforce/att-confirms-73m-customers-affected-data-leak; https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last visited July 13, 2024)

phone numbers, postal addresses, and Social Security numbers.[20] Based on AT&T's preliminary analysis, the data appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders. AT&T claims there is no evidence this was the result of unauthorized access to its systems.[21]

B. AT&T's Breached Data Was Hosted on Snowflake's Data Cloud

41. An AT&T spokesperson confirmed that the data was exposed "on 'AI data cloud' provider Snowflake[.]" AT&T also confirmed "that the Snowflake breach is unrelated to the leak involving the data of 73 million current and former subscribers" from earlier this year.[22]

42. Snowflake provides digital warehouses, known as "Snowflake Data Clouds" for its thousands of clients around the world, and as a result has access to, stores, and maintains huge datasets of Personal Information of its corporate clients' customers and employees. Snowflake's corporate clients include AT&T and many others.[23]

43. In or around mid-April 2024, an unauthorized party or parties gained

---

[20] *Ibid*.
[21] *Ibid*.
[22] https://arstechnica.com/tech-policy/2024/07/nearly-all-att-subscribers-call-records-stolen-in-snowflake-cloud-hack/ (last visited July 12, 2024)
[23] https://www.snowflake.com/en/customers/all-customers/ (last visited July 12, 2024)

access to at least 165 Snowflake customer accounts stealing customer and employee data from AT&T, Ticketmaster, Santander, QuoteWizard, and Advanced Auto Parts, among others.[24]

44. Google-owned cybersecurity incident response firm, Mandiant, which Snowflake retained to help it investigate the incident, attributed the breach to an as-yet-uncategorized cybercriminal group tracked as UNC5537. Mandiant's researchers say the hackers are financially motivated and have members in North America and at least one member in Turkey. Data of some of Snowflake's over 160 corporate customers has been published on known cybercrime forums.[25]

C. Mandiant Confirms That Failure to Implement Multi-Factor Authentication Was a Significant Factor in the Data Breach

45. Mandiant revealed that the threat campaign was successful because "the impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password."[26]

46. MFA is a simple yet robust security system that requires more than one

[24] https://www.bleepingcomputer.com/news/security/advance-auto-parts-stolen-data-for-sale-after-snowflake-attack/; https://www.wired.com/story/snowflake-breach-advanced-auto-parts-lendingtree/ (last visited July 13, 2024)
[25] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion (last visited July 13, 2024)
[26] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion (last visited July 13, 2024)

method of authentication from independent categories of credentials (e.g., a username/password and confirmation link sent via email).

47. Infamous threat actors, known by the handle "ShinyHunters," boasted to journalists that the Data Breach was enabled by the lack of MFA enforcement.[27]

48. MFA administrator enforcement is the industry standard, according to Ofer Maor, cofounder and Chief Technology Officer of data security investigation firm Mitiga.[28] He notes that "most SaaS (soft-as-a-service) vendors, once deployed as an enterprise solution, allow administrators to enforce MFA… they require every user to enroll in MFA when they first login and make it no longer possible for users to work without it." A data security firm's principal simply noted it is "surprising that the built-in account management within Snowflake doesn't have more robust capabilities like the ability to enforce MFA." [29]

49. Snowflake blames the data thefts on its customers – such as AT&T here, who did not require MFA to secure their Snowflake accounts. However, Snowflake did not enforce or require its corporate customers to use MFA. Here, Defendants' joint failure to implement the most basic cybersecurity feature

[27] https://www.wired.com/story/epam-snowflake-ticketmaster-breach-shinyhunters/ (last visited July 13, 2024)
[28] https://www.itpro.com/security/cyber-attacks/with-hundreds-of-snowflake-credentials-published-on-the-dark-web-its-time-for-enterprises-to-get-mfa-in-order (last visited June 28, 2024).
[29] https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say (last visited June 28, 2024)

(enabling/enforcing MFA) was the cause of this Data Breach.

50. Snowflake, as a data cloud service provider, is aware that certain basic security measures are critical to protecting sensitive information and that these include implementing MFA requirements and enabling administrator controls to mandate MFAs for its users.

51. AT&T likewise knows the importance of MFA. According to AT&T, "[t]he majority of data breaches are caused by brute force attacks on credentials."[30] AT&T even has its own MFA application, AT&T MFA, which it describes as "AT&T's secure multi-factor authenticator that significantly improves both business and personal account login security."[31]

52. Yet neither Snowflake nor AT&T took any measures to ensure that the sensitive information located on Snowflake's cloud was fully protected. By implementing a policy to enable MFA and even allowing the companies who use Snowflake's cloud servers to enforce MFA features may have prevented this Data Breach.

53. Shortly after its security incident Snowflake implemented significant changes to its MFA practices, including giving administrators the option to make MFA mandatory, adding more security customization options, and introducing a

[30]https://cdn-cybersecurity.att.com/docs/product-briefs/att-multi-factor-authenticator.pdf (last visited July 13, 2024)
[31] https://apps.apple.com/us/app/at-t-mfa/id6444501887 (last visited July 13, 2024)

new platform for monitoring, and enforcing MFA policies.[32]

54. Specifically, administrators will be allowed to push MFA on all users, as well as those using Single Sign-On (SSO), or just specific, individual accounts. Users that log into their Snowflake accounts will be prompted to activate the new feature. If they decline, they will get another prompt in three days.[33] Snowflake also introduced the Snowflake Trust Center, where admins can monitor the adherence to MFA policies. Part of that feature is the Trust Center Security Essentials scanner package, which looks for MFA compliance, as well as the use of network policies. Snowflake also introduced the Trust Center CIS Benchmark scanner package, which evaluates the account against the CIS Snowflake Foundations Benchmark. These scanners can detect overprivileged users, accounts that have not logged in for more than three months, and more.[34] All of these steps reasonably should have been implemented prior to the Data Breach.

D. Defendants Promised to Safeguard Customers' Personal Information

55. AT&T collects a vast amount of data from its customers. AT&T's Privacy Notice identifies the data it collects as including:

[32] https://www.techradar.com/pro/security/snowflake-is-bringing-in-some-big-mfa-changes-following-recent-security-incidents (last visited July 13, 2024)
[33] *Ibid*.
[34] *Ibid.*

Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information (https://www.att.com/consent/cpni/)[35]

Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number.

Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working.

Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites.

Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information.

Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric

[35] AT&T explains: "We use Customer Proprietary Network Information (CPNI) to offer new types of products and services we think you'd like from AT&T and our affiliates. CPNI is information about your telecommunications and VoIP (internet phone) services from us, including what plans you subscribe to, how you use these services and details such as who you have called." https://www.att.com/consent/cpni/ (last visited July 14, 2024)

> Information Privacy Notice (/privacy/privacy-notice/biometrics.html)
>
> **Third-party information**. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.[36]

56. According to AT&T "All these types of information are considered Personal Information when they can reasonably be linked to you as an identifiable person or household. For instance, information is personal when it can be linked to your name, account number or device."[37]

57. AT&T promises to provide confidentiality and adequate security for the data it collects from customers, including Plaintiffs and Class Members, through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements. AT&T' Privacy Notice provides:

> **Data retention and security**
>
> We keep your information as long as we need it for business, tax or legal purposes. We set our retention periods based on things like what type of personal information it is, how long it's needed to operate the business or provide our products and services, and whether it's subject to contractual or legal obligations. These obligations might be ongoing litigation, mandatory data retention laws or government orders to preserve data for an investigation. After that, we destroy it by making it unreadable or indecipherable.

[36] https://about.att.com/privacy/privacy-notice.html (last visited July 14, 2024)
[37] *Ibid*.

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.
>
> No security measures are perfect. We can't guarantee that your information will never be disclosed in a manner inconsistent with this notice. If a breach occurs, we'll notify you as required by law.[38]

58. AT&T's Privacy Policy further states that while it shares customers' Personal Information with certain third parties AT&T requires those parties to protect that information consistent with its Privacy Policy:

> **How we share your information**
>
> As described in the following paragraphs, AT&T shares information within our own AT&T companies and affiliates. We also share with non-AT&T companies.
>
> *** *** ***
>
> **Non-AT&T companies providing a service**.
>
> We use suppliers for services like marketing and mailing bills. When we share your information with suppliers, we require them to use it only for the intended purpose and to protect it consistent with this notice.
>
> **Non-AT&T companies or entities where authorized or required by law. [¶]** This can happen when we:

[38] *Ibid.*

> ● Comply with court orders, subpoenas, and lawful discovery requests, and as otherwise authorized or required by law. Like all companies, we must comply with legal requirements. You can learn more in our Transparency Report (/privacy/transparencyreport.html).
>
> ● Detect and prevent fraud.
>
> ● Provide or obtain information related to payment for your service.
>
> ● Route your calls or other communications, like connecting calls or text messages with other carrier networks.
>
> ● Ensure network operations and security, defend against legal claims and enforce our legal rights.
>
> ● Notify, respond, or provide information (including location) to an appropriate governmental entity in emergency circumstances such as immediate danger of death or serious physical injury.
>
> ● Alert the National Center for Missing and Exploited Children to information concerning child pornography if we become aware through the provision of our services.
>
> ● Share the names, addresses and telephone numbers of non-mobile phone customers with phone directory publishers and directory assistance services as required by law. We honor your request for non-published or non-listed numbers.
>
> ● Provide name and phone number for wireline and wireless Caller ID and related services like Call Trace.[39]

59. Additionally, AT&T's July 12, 2024 notice of "Unlawful access of customer data" posted on its website promises: "We hold ourselves to a high

[39] *Ibid*.

standard and commit to delivering the experience that you deserve. We constantly evaluate and enhance our security to address changing cybersecurity threats and work to create a secure environment for you. We invest in our network's security using a broad array of resources including people, capital, and innovative technology advancements."[40]

60. Snowflake is one of the largest digital warehouse providers in the United States and contracts with thousands of companies to securely store customers and employes' data on its Snowflake Data Cloud. As such, Snowflake is responsible for developing and maintaining environments which collects and processes personal data for hundreds of millions of Americans.

61. Snowflake included privacy policies and commitments to maintain the confidentiality of data stored in its digital warehouses as terms of contracts with its corporate clients. Through contract terms and representations to its corporate clients and the public Snowflake promised to take specific measures to protect Personal Information of Plaintiffs and Class Membrs and as such they are intended third-party beneficiaries of Snowflake's contracts.[41]

62. Snowflake's Privacy Notice from November 24, 2023, prior to its

[40] https://www.att.com/support/article/my account/000102979?source=EPcc000000000000U (last visited July 12, 2024)
[41]https://web.archive.org/web/20240218162854/https://www.snowflake.com/privacy-policy/ (last visited July 14, 2024)

modification on March 6, 2024, states:

> We provide the Service to our customers under an agreement with them and solely for their benefit. Our customers designate which of their personnel (including third party contractors, agents, etc.) are authorized as users of the customer's Service account ("Authorized Users"). Authorized Users may access and use the Service from all over the world, subject to the agreement between Snowflake and the customer as well as any applicable laws.
>
> This Notice does not apply to the content that our customers and their Authorized Users upload and store in the Service ("Customer Content"). Snowflake processes Customer Content solely on behalf of the customer and that customer is responsible for the collection and use of your data. Because of this, that customer's privacy notice (and not this Notice) will apply to the customer's collection and use of Customer Content. Therefore, for any queries related to your data in Customer Content, you should refer to their privacy notice and direct any queries to them. The customer's agreement with Snowflake governs our use of and processing of Customer Content. For information about our data collection and use regarding Authorized Users use of our Service see the "When using the Service" Sub-section of the "Information We Automatically Collect" Section below.[42]

63. Snowflake's Privacy Policy promises:

> **Security of Your Personal Information**
>
> We take all reasonable and appropriate steps to protect your personal information in an effort to prevent loss, misuse, and

[42] *Ibid.*

> unauthorized access, disclosure, alteration and destruction. We use appropriate technical and organizational measures to protect your personal information which may include: physical access controls, encryption, internet firewalls, intrusion detection and network monitoring depending on the nature of the information and the scope of processing. Our staff, who may have access to your personal information, are required to keep your personal information confidential.[43]

64. Snowflake received a financial benefit – a fee for its services which included storing and protecting its data cloud servers to ensure that Plaintiffs' and Class Members' Personal Information would be protected.

65. Defendants assumed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs' and Class Members' Personal Information against unauthorized access and disclosure. Defendants were aware that the large data files stored on Snowflake's servers contain sensitive information of millions of individuals – the clients/employees of thousands of companies with whom Snowflake contracted.

66. Snowflake's responsibility was to protect its cloud servers and the sensitive files stored on its servers. At least a partial (if not full) payment for Snowflake's services was attributed to protecting the files and sensitive information

[43] *Ibid*.

on its cloud platforms.

67. Snowflake disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure Plaintiff and Class Members' data was protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Personal Information; failing to take standard and reasonably available steps to prevent the Data Breach, including but not limited to requiring corporate clients like AT&T to implement MFA on its Snowflake Data Cloud; failing to properly train its staff and employees on proper security measures; and failing to properly monitor its computer network and systems that housed the Personal Information.

68. AT&T's responsibility was to protect the Personal Information of Plaintiffs and Class Members by implementing and ensuring its third-party service providers implemented sufficient security measures to protect Plaintiffs and Class Members' Personal Information, including but not limited to MFA.

69. AT&T breached its duties and disregarded the rights of Plaintiffs and the Class Members by intentionally, willfully, recklessly, or negligently, *inter alia*, failing to implement proper and reasonable measures to safeguard individuals' (whose information it was required to protect) Personal Information; failing to take available and necessary steps to prevent unauthorized disclosure of data; and failing

to follow minimum industry standards and protocols, including implementing MFA on its Snowflake Data Cloud account.

70. Plaintiffs and other customers paid AT&T for its services. At least a partial payment for AT&T's services was attributed to protecting Plaintiffs' and Class Members' information in AT&T's possession, including the information released to criminals here.

71. As a result of Defendants' inadequate security and breach of their duties and obligations, the Personal Information of Plaintiffs and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiffs and Class Members have suffered injuries as a direct and proximate result of Defendants' conduct.

E. Personal Information Is a Valuable Property Right

72. Personal Information, particularly personally identifiable information ("PII") is a valuable property right.[44] In a Federal Trade Commission roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be

[44] https://www.researchgate.net/publication/283668023 (last visited June 28, 2024)

> commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[45]

73. The value of PII as a commodity is measurable.[46] "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[47]

74. "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[48] It is estimated that American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[49] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web" for many years.

75. As a result of its real value identity thieves and cyber criminals often ransom stolen data demanding companies pay large sums of money under the threat of public disclosure or its being put up for sale on the Dark Web.

---

[45]https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable (last visited July 14, 2024)
[46]http://www.medscape.com/viewarticle/824192 (last visited July 14, 2024)
[47] *See* John T. Soma *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (citations omitted).
[48] https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited June 28, 2024)
[49] https://www.iab.com/news/2018-state-of-data-report/ (last visited June 28, 2024).

76. The criminals who compromised Snowflake's corporate accounts are seeking millions of dollars in exchange for the stolen information. For instance, Ticketmaster data is being sold for $500,000[50] and Advance Auto Parts data is being sold for $1.5 million on the Dark Web.[51]

77. Further, consumers place a high value on the privacy of their data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[52] Here, Plaintiff and Class Members paid a price premium to AT&T dedicated to securing and protecting their data.

78. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

F. Defendants Knew or Should Have Known They Were High Risk Targets For Data Thieves

79. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared

[50]https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale/ (last visited June 28, 2024)
[51]https://www.bleepingcomputer.com/news/security/advance-auto-parts-stolen-data-for-sale-after-snowflake-attack/ (last visited June 28, 2024)
[52] https://www.jstor.org/stable/23015560?seq=1 (last visited June 28, 2024)

for, a potential attack.[53] The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency ("CISA"), State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendants on notice, long before the Data Breach, that (1) cybercriminals are targeting large, public companies such as Snowflake and AT&T; (2) cybercriminals are ferociously aggressive in their pursuit of large collections of Personal Information like that in possession of Defendants; (3) cybercriminals are selling large volumes of Personal Information and corporate information on Dark Web portals; (4) the threats are increasing.

80. Had each Defendant been diligent and responsible, it would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key ***avoidable*** causes for security incidents are:

- Lack of complete assessment, including internal, third-party, and **cloud-based systems and services**;
- **Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports**;
- Misconfigured devices/servers;
- **Unencrypted data and/or poor encryption key management and**

[53] https://www.law360.com/articles/1220974 (last visited June 28, 2024)

safeguarding;

- Use of end-of-life (and thereby unsupported) devices, operating systems and applications;
- Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;
- Failure to block malicious email; and
- Users succumbing to business email compromise (BEC) and social exploits.[54]

81. Therefore, Defendants could have prevented this breach if they addressed the common avoidable causes for data breaches – including enabling and requiring the MFA features.

82. AT&T is well aware the data it collects and stores about its customers is a high target for data thieves. This underscores the need for immediate injunctive and other relief to protect millions of consumers across the United States. Below is a timeline of AT&T data breaches:

> **February 2024: AT&T Addresses Data Set Released on the Dark Web**
> AT&T confirms that personal data belonging to 73 million customers was leaked on the Dark Web. The data may have included Social Security numbers, passcodes, full names, email addresses, mailing addresses, phone numbers, dates of birth, and AT&T account numbers. According to AT&T the data set appears to be from 2019 or earlier, impacting approximately 7.6

[54] https://www.proofpoint.com/us/securityawareness/post/ota-report-indicates-93-security-breaches-are-preventable (last visited June 28, 2024).

million current AT&T account holders and 65.4 million former account holders. AT&T states it has no evidence that the data theft was from unauthorized access to its systems.[55]

March 2023: AT&T Notifies 9 Million Customers Following Attack on Vendor

AT&T notified roughly 9 million customers that their data had been compromised following an attack on a third-party vendor. AT&T described the exposed data as "Customer Proprietary Network Information," including data on customers' wireless plans and payment amounts.

August 2022: Stolen Data Discovered on 23 Million AT&T Customers

Hold Security – a cybersecurity firm – discovered stolen data featuring the names, Social Security numbers, dates of birth, and more information on approximately 23 million Americans. After analyzing the data Hold Security determined it likely relates to current or former AT&T customers. AT&T claimed this breach was potentially connected to a data incident at another company.

July 2020: US Department of Justice Charges AT&T Employees in Massive Phone Unlocking Scheme

Between 2012 and 2017, a number of AT&T employees at a call center in Bothell, Washington, were bribed to install malware and install unauthorized hardware as part of a phone unlock scam. Two men paid more than $1 million in bribes to compromise AT&T's internal networks and have phones unlocked in exchange for payments. It was estimated the hackers unlocked over 2 million devices.

April 2014: Third-Party Vendor Uses Personal Data to Unlock Phones

An AT&T wireless data breach relating to the activities of three third-party vendor employees. The employees accessed

[55] https://www.att.com/support/article/my-account/000101995?bypasscache=1/?source=EPcc000000000000U (last visited July 14, 2024)

> personal data on customer accounts without authorization, giving them the ability to view details like birth dates, Social Security numbers, and limited call data such as destination numbers, times and dates of calls, and durations. The employees were requesting codes to unlock AT&T mobile devices, making them usable on other networks. At least 500 customers were affected.
>
> **2014: AT&T Insider Data Breach Exposes Information on 280k Customers**
> In 2013 and 2014, employees at AT&T call centers operating in Colombia, Mexico, and the Philippines exposed sensitive customer data to third parties. The data included the names and Social Security numbers (either full or partial) of approximately 280,000 AT&T customers. In April 2015, the FCC fined AT&T $25 million for the breach.[56]

83. Snowflake is also well aware of its being a high value target for cybercriminals. In March 2023, the FTC sought comments from Computing Providers (like Snowflake) and their impact on end users, customers, companies, and other businesses across the economy (like AT&T) on the business practices of cloud computing providers including issues related to the market power of these companies, impact on competition, and potential security risks.[57]

84. The FTC acknowledged it had brought several cases against companies that failed to implement basic security safeguards to protect data they stored on third-

[56] https://firewalltimes.com/att-data-breaches/#:~:text=The%20most%20recent%20AT%26T%20data,on%20a%20third%2Dparty%20vendor (last visited July 14, 2024)
[57] https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-seeks-comment-business-practices-cloud-computing-providers-could-impact-competition-data (last visited July 14, 2024)

party cloud computing services and that the FTC has issued guidance to businesses on steps they can take to secure and protect data stored in the cloud.[58]

85. FTC guidance to companies like AT&T and Snowflake for the use of cloud services includes the following six tips: (1) take advantage of the security features offered by cloud service companies; (2) take regular inventories of what you keep in the cloud; (3) do not store personal information when it is not necessary; (4) consider encrypting rarely used data; (5) pay attention to credible warning; (6) security is your responsibility.[59]

G. Plaintiffs and the Class Have Suffered Injury as a Result of Defendants' Data Mismanagement

86. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiffs' and Class Members' Personal Information has been and is now in the hands of an unauthorized third-party that may include thieves, unknown criminals, and other potentially hostile individuals or entities. Plaintiffs and Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

87. Although personally identifying information such as names was not disclosed in the Data Breach, AT&T admits that "[w]hile the data doesn't include

[58] *Ibid*.
[59] https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing (last visited April 14, 2024)

customer names, there are often ways to find a name associated with a phone number using publicly available online tools."[60]

88. AT&T recognizes that Plaintiffs and Class Members face an increased risk of phishing and smishing attacks, and other online fraud and online threats because of the Data Breach warning Plaintiffs and Class Members:[61]

What can I do to help protect myself from phishing, smishing, and other online fraud?

- Only open text messages from people that you know and trust.
- Don't reply to a text from an unknown sender with personal details.
- Go directly to a company's website. Don't use links included in a text message. Scammers can build fake websites using forged company logos, signatures, and styles.
- Make sure a website is secure by looking for the "s" after the http in the address. You can also look for a lock icon at the bottom of a webpage.

Find more tips and info on CyberAware, our website dedicated to raising awareness and educating customers on fraud and cyber threats.

What can I do to help protect myself from online threats?

As a general rule, we recommend that you remain cautious of any phone call or text request asking you for personal, account, or credit card details. If you suspect:

- **Suspicious text activity:** Do not reply. Learn how to forward the text to AT&T so we can assist you. Forwarded messages are free and won't count toward your text plan.
- **You are a target of fraud on your AT&T wireless number:** Report it to our Fraud team. If you suspect fraud on another account, call the customer service number on your bill for help.

89. Plaintiffs and members of the Class must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive

[60] https://www.att.com/support/article/my-account/000102979?source=EPcc000000000000U (last visited July 14, 2024)
[61] *Ibid*.

account; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

90. For instance, as a result of this Data Breach, and AT&T's express warnings, Plaintiff Woon must continue to devote time and energy to review all of her financial activity and monitor her credit. She must continue to regularly change logins and password information on various personal accounts which could subject her to a monetary loss, carefully scrutinizing and screening phone calls, emails, and other communications, and must continue to use identity theft protection and credit monitoring services.

91. Plaintiffs have also overpaid AT&T (and thus, in turn to Snowflake) for its services, a portion of which was dedicated to protecting Plaintiffs' Personal Information and activities (such as call logs/text messages) while using AT&T's services.

92. Once Personal Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years because of Defendants' conduct. Further, the value of Plaintiffs' and Class Members' Personal Information has been diminished

by its exposure in the Data Breach.

93. Plaintiffs and members of the Class suffered actual injury from having Personal Information compromised as a result of Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their Personal Information, a form of property that Defendants obtained from and about Plaintiffs and Class Members; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud through phishing, smishing, and other hostile attacks.

94. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiffs' and Class Members' Personal Information has been and is now in the hands of unauthorized third-party criminals. Plaintiffs and Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

95. Plaintiffs and Class Members have had their Personal Information stolen by cybercriminals and have experienced and will continue to experience emotional pain and mental anguish and embarrassment. The criminals now know Plaintiffs' and Class Members' detailed call log activities for 6 months – which depict who Plaintiffs and the Class Members interacted with and the associated metadata for those interactions, as well as location data for at least a subset of Class

Members. This information can be used to perpetrate phishing scams, spoof phone numbers of the loved ones or corporate companies with whom Plaintiffs and Class Members interact with to gain access to Plaintiffs' and Class Members' financial resources. Furthermore, this information consists of the information that cannot be changed, and is thus, of tremendous value to criminals.

96. Plaintiffs and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted (including Plaintiffs here) are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim for cybercrimes for years to come.

97. Furthermore, the information Defendants failed to protect here, can be aggregated and combined with the data from other data breaches (such as AT&T's earlier data breach). Thus, this key information regarding Plaintiffs' and Class Members' detailed interaction for a long period of time – six months – is even more valuable to thieves and more damaging to victims, which was not available to them prior to this data breach.

H. Defendants Failed to Comply with FTC Guidelines

98. Defendants are prohibited by the Federal Trade Commission Act (the "**FTC Act**"), 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "**FTC**") has concluded that a company's failure to maintain reasonable and appropriate data

security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

99. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

100. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[62] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event

[62] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited June 28, 2024)

of a breach.[63]

101. The FTC further recommends that companies not maintain personal information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

102. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

103. Furthermore, as discussed above, the FTC has issued guidance specifically to the entities which use cloud-based services, and reminded them that securing the information on the cloud-based services is their corporate responsibility.

---

[63] *Ibid.*

CLASS ACTION ALLEGATIONS

104. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("**the Class**").

105. Plaintiffs propose the following Class and Subclasses subject to amendment(s) as appropriate:

Nationwide Class

> All individuals residing in the United States whose Personal Information was compromised as a result of the Data Breach.

Florida Subclass

> All individuals residing in Florida whose Personal Information was compromised as a result of the Data Breach. (the "Florida Subclass").

California Subclass

> All individuals residing in California whose Personal Information was compromised as a result of the Data Breach. (the "California Subclass").

106. Collectively, the Nationwide Class, the Florida Subclass and the California Subclass are referred to as the "Class."

107. Excluded from the Class are Defendants' officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their

families and members of their staff.

108. **Numerosity:** The members of the Class are so numerous that joinder of all of them is impracticable – millions of individuals have been affected by this Data Breach.

109. **Predominance of Common Questions**. There exist questions of law and fact common to the Class, which predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Personal Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Personal Information;

f. Whether Defendants were s subject to (and breached) the FTC Act;

g. Whether Defendants breached their duty to Class Members to safeguard their Personal Information

h. Whether computer hackers obtained Class Members' Personal Information in the Data Breach;

i. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' acts breached an implied contract they formed with Plaintiffs and the Class Members;

l. Whether Defendants were unjustly enriched to the detriment of Plaintiffs and the Class;

m. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

110. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Personal Information, like that of every other Class Member, was compromised in the Data Breach.

111. **Adequacy:** Plaintiffs are adequate representatives for the Class because their interests do not conflict with the interests of the Class that they seek to represent. Plaintiffs have retained counsel competent and highly experienced in complex class action litigation and who intends to prosecute this action vigorously.

The interests of the Class will be fairly and adequately protected by Plaintiffs and their experienced counsel.

112. **Superiority:** A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and members of the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them by Defendants. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based upon, *inter alia*, the records AT&T maintains regarding Plaintiffs and Class Members.

113. Defendants have acted on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

CLAIMS FOR RELIEF

COUNT 1
NEGLIGENCE
(On Behalf of Plaintiffs and Each Class Against All Defendants)

114. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

115. Defendants owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their Personal Information in Defendants' possession, custody, or control.

116. Defendants knew, or should have known the risks of collecting and storing Plaintiffs' and all other Class Members' Personal Information and the importance of maintaining secure systems. Defendants knew, or should have known, of the vast uptick in data breaches in recent years. Defendants had a duty to protect the Personal Information of Plaintiffs and Class Members.

117. Given the nature of Defendants' businesses, the sensitivity and value of the Personal Information they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring, which Defendants had a duty to prevent.

118. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor,

and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Personal Information entrusted to it—including Plaintiffs' and Class Members' Personal Information.

119. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' Personal Information to unauthorized individuals.

120. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiffs and the Class Members, their Personal Information would not have been compromised.

121. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii)

improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well- established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and Each Class Against All Defendants)

122. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

123. Defendants' duties arise from Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure Personal Information.

124. Defendants violated Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class Members' Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information it obtains and stores, and the foreseeable consequences of a

data breach involving Personal Information including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

125. Defendants' violations of Security Rules and Section 5 of the FTCA constitute negligence per se.

126. Plaintiffs and Class Members are within the class of persons that Security Rules and Section 5 of the FTCA were intended to protect.

127. The harm occurring because of the Data Breach is the type of harm Security Rules and Section 5 of the FTCA were intended to guard against.

128. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' Personal Information to unauthorized individuals.

129. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendants' violations of Security Rules and Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying

expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and Each Class Against All Defendants)

130. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

131. Plaintiffs and Class Members either directly or indirectly gave Defendants their Personal Information in confidence, believing that Defendants would protect that information. Plaintiffs and Class Members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiffs' and Class Members' Personal Information created a fiduciary relationship between Defendants and Plaintiffs and Class Members. Considering this relationship, Defendants must act primarily for the benefit of Plaintiffs and Class Members, which includes safeguarding and protecting Plaintiffs' and Class Members' Personal Information.

132. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and

Class Members upon matters within the scope of their relationship. Defendants breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' Personal Information, failing to safeguard the Personal Information of Plaintiffs and Class Members they collected.

133. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Personal Information which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Personal Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and Each Class Against all Defendants)

134. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

135. Plaintiffs and Class Members conferred a monetary benefit upon

Defendants in the form of monies paid for services—namely, they provided and entrusted AT&T with their valuable Personal Information. AT&T, in turn, entrusted Plaintiffs' and the Class Members' information to Snowflake, and on behalf of Plaintiffs and the Class paid a fee to Snowflake for its data storage services. Therefore, AT&T and Snowflake have been receiving payments (at least in part) intended to protect Plaintiffs' and Class Members' information.

136. AT&T funds its data security measures (including to payments to Snowflake) from payments made by and on behalf of Plaintiffs and the Class Members.

137. AT&T paid to Snowflake (on behalf of Plaintiffs and the Class) for its data storage services, a portion of which was intended to provide them with a reasonable level of data security from both AT&T and Snowflake in order to protect Plaintiffs' and the Class Members' Personal Information.

138. In exchange for their payment, Plaintiffs and Class Members were entitled to reasonable measures to protect their Personal Information.

139. Defendants appreciated, accepted and retained the benefit bestowed upon them under inequitable and unjust circumstances arising from their conduct toward Plaintiffs and Class members as described herein –namely, (a) Plaintiffs and Class members conferred a benefit on Defendants, and Defendants accepted or retained that benefit; and (b) Defendants used Plaintiffs' and Class Members'

Personal Information for business purposes.

140. Defendants failed to secure Plaintiffs' and Class Members' Personal Information and, therefore, did not provide full compensation for the benefit provided on behalf of Plaintiffs and Class Members.

141. Defendants acquired the Personal Information through inequitable means in that it failed to disclose its inadequate security practices previously alleged.

142. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

143. Under the circumstances, it would be unjust and unfair for Defendants to be permitted to retain any of the benefits conferred by or on behalf of Plaintiffs and the Class.

144. Under the principles of equity and good conscience, Defendants should not be permitted to retain the Personal Information belonging to Plaintiffs and Class Members because Defendants failed to implement the data management and security measures that industry standards mandate.

145. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received on behalf of and for the benefit of Plaintiffs and the Class.

COUNT V
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and Each Class Against Snowflake)

146. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

147. Defendant Snowflake entered into contracts with its various corporate clients, including AT&T to provide data storage services and maintain secure data cloud systems. These contracts were made expressly for the benefit of Plaintiffs and Class Members, who were customers and/or employees of AT&T. In order to effectuate offered services and upon information and belief as to the exact terms of the contract, Defendant Snowflake agreed to collect, store, and protect Plaintiffs' and Class Members' Personal Information.

148. Thus, the benefit of collection, protection, and storage of the Personal Information was the direct, intended, and primary objective of the contracting parties.

149. Defendant Snowflake breached its contract with AT&T when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' Personal Information.

150. Defendant Snowflake knew that if it were to breach its contracts, the harm would befall its clients' customers and employees for whom the benefit was intended to confer. As such, Defendant Snowflake's failure to uphold the terms of

its contract and allow for the Data Breach has foreseeably harmed Plaintiffs and the Class.

151. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial, along with their costs including attorneys' fees incurred.

COUNT VI
INVASION OF PRIVACY
(*On Behalf of Plaintiffs and Each Class Against All Defendants*)

152. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

153. Plaintiffs and Class Members have a legally protected privacy interest in their Personal Information that Defendants required them to provide and/or allow them to store.

154. Plaintiffs and Class Members reasonably expected their Personal Information would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

155. Defendants unlawfully invaded the privacy rights of Plaintiffs and Class Members by (a) failing to adequately secure their Personal from disclosure to unauthorized parties for improper purposes; (b) leaving their Personal Information exposed to unauthorized parties in a manner that is highly offensive

to a reasonable person; and (c) leaving their Personal Information exposed to unauthorized parties without the informed and clear consent of Plaintiffs and Class Members. This invasion into the privacy interest of Plaintiffs and Class Members is serious and substantial.

156. In failing to adequately secure Plaintiffs' and Class Members' Personal Information, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiffs and Class Members.

157. Defendants violated Plaintiffs' and Class Members' right to privacy under the common law as well as under state and federal law.

158. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiffs' and Class Members' Personal Information has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and the proposed Class have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

COUNT VII
BREACH OF CONTRACT
(*On Behalf of Plaintiffs and Each Class Against AT&T*)

159. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

160. As a condition of purchasing products and services from AT&T, Plaintiffs agreed to the terms in AT&T's Privacy Notice.[64]

161. The Privacy Notice formed a contract between AT&T and Plaintiffs and Class Members.

162. Under this contract AT&T promised that it "work[s] hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information."[65]

[64] https://about.att.com/privacy/privacy-notice.html (last visited July 14, 2024)
[65] *Ibid.*

163. AT&T also promised that while it shares customers' Personal Information with certain third parties it requires those parties to protect that information consistent with its Privacy Notice.[66]

164. Additionally, AT&T's July 12, 2024 notice of "Unlawful access of customer data" posted on its website promises: "We hold ourselves to a high standard and commit to delivering the experience that you deserve. We constantly evaluate and enhance our security to address changing cybersecurity threats and work to create a secure environment for you. We invest in our network's security using a broad array of resources including people, capital, and innovative technology advancements."[67]

165. In return, Plaintiffs and Class members promised, among other things, to allow AT&T to collect and share their Personal Information.[68]

166. Plaintiffs and Class Members performed their obligations under the Privacy Notice when they provided their Personal Information to AT&T in relation to their purchasing and using AT&T cellular products and services.

167. By allowing unauthorized users to gain access to Plaintiffs' and Class Members' Personal Information through the Data Breach, AT&T breached

---

[66] *Ibid*.
[67] https://www.att.com/support/article/my account/000102979?source=EPcc000000000000U (last visited July 12, 2024)
[68] https://about.att.com/privacy/privacy-notice.html (last visited July 14, 2024)

its contractual obligations. As a result, AT&T failed to comply with its own policies, including its Privacy Notice, and applicable laws, regulations and industry standards for data security and protecting the confidentiality of Plaintiffs' and Class Members' Personal Information. AT&T's breach of contract also violated California Business and Professions Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of its posted privacy policy.

168. By failing to fulfill its contractual obligations under its Privacy Policy, AT&T failed to confer on Plaintiffs and Class Members the benefit of the bargain, causing them economic injury.

169. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

COUNT VIII
BREACH OF IMPLIED CONTRACT
(*On Behalf of Plaintiffs and Each Class Against AT&T*)

170. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

171. Defendant AT&T provided Plaintiffs and Class Members with an implied contract to protect and keep their Personal Information private.

172. Plaintiffs and Class Members would not have provided their Personal Information to Defendant AT&T or its subsidiaries or contractors, but for Defendant AT&T's implied promises to safeguard and protect their information.

173. Plaintiffs and Class Members performed their obligations under the implied contract when they provided their Personal Information to Defendant AT&T for cellular and other services provided by Defendant AT&T.

174. Defendant AT&T breached the implied contracts with Plaintiffs and Class Members by failing to protect and keep private their Personal Information.

175. As a direct and proximate result of Defendant AT&T's breach of its implied contracts, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

COUNT IX
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of the California Plaintiff and Subclass Against All Defendants)

176. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

177. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused

the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

178. In the course of conducting its business, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class members' Personal Information, and by violating the statutory and common law alleged herein. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

179. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendants' practices are also contrary to legislatively declared and public policies that seek to protect Personal Information and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as

reflected by laws such as the Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45). The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

180. The UCL also prohibits any "fraudulent business act or practice." Defendants' above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

181. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Personal Information, (iv) statutory damages, (v) deprivation of the value of their Personal Information, for which there is a well-established national and international

market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

182. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves individually, Class Members, and the general public, also seek restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Personal Information entrusted to them, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

COUNT X
VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT ("CLRA), California Civil Code §§ 1750, *et seq*.
(On Behalf of the California Plaintiff and Subclass Against All Defendants)

183. Plaintiff Woon re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

184. The CLRA prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of goods.

185. Defendants' unlawful conduct described herein was intended to

increase sales to the consuming public and violated and continue to violate Section 1770(a)(5), (a)(7), and (a)(9) of the CLRA by representing that the products and services have characteristics and benefits which they do not have.

186. Defendants fraudulently deceived Plaintiff Woon and the California Subclass by representing that their products and services have certain characteristics, benefits, and qualities which they do not have, namely data protection and security. In doing so, Defendants intentionally misrepresented and concealed material facts from Plaintiff Woon and the California Subclass, specifically by advertising secure technology when Defendants in fact failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiff Woon and the California Subclass and depriving them of their legal rights and money.

187. Defendants' claims about the products and services led and continues to lead consumers like Plaintiff to reasonably believe that Defendants have implemented adequate data security measures when Defendants in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access consumers' Personal Information.

188. Defendants knew or should have known that adequate security measures were not in place and that consumers' Personal Information was

vulnerable to a data breach.

189. Plaintiff Woon and the California Subclass have suffered injury in fact as a result of and in reliance upon Defendants' false representations.

190. Plaintiff Woon and the California Subclass would not have purchased the products or used the services, or would have paid significantly less for the products and services, had they known that their Personal Information was vulnerable to a data breach.

191. Defendants' actions as described herein were done with conscious disregard of Plaintiffs' rights, and Defendants were wanton and malicious in their concealment of the same.

192. Plaintiff Woon and the California Subclass have suffered injury in fact and have lost money as a result of Defendants' unfair, unlawful, and fraudulent conduct. Specifically, Plaintiffs paid for products and services advertised as secure, and consequentially entrusted Defendants with their Personal Information, when Defendants in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the California Subclass would not have purchased the products and services or would not have provided Defendants with their Personal Information, had they known that their Personal Information was vulnerable to a data breach.

193. Defendants should be compelled to implement adequate security

practices to protect consumers' Personal Information. Additionally, Plaintiffs and the members of the California Subclass lost money as a result of Defendants' unlawful practices.

194. At this time, Plaintiff Woon seeks injunctive relief under the CLRA pursuant to Cal. Civ. Code 1782(d); but she anticipates the need to amend the complaint and seek restitution.

COUNT XI
Violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), (Fla. Stat. §§ 501.201, et seq.)
(On Behalf of the Florida Plaintiff and Subclass Against All Defendants)

195. Plaintiff Olivieri re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

196. Defendants engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendants obtained the Personal Information of Plaintiff Olivieri and the Florida Subclass through advertising, soliciting, providing, offering, and/or distributing goods and services to Plaintiff Olivieri and the Florida Subclass or on their behalf and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

197. As alleged in this Complaint, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard Personal Information;

b. failure to make only authorized disclosures of Plaintiff Olivieri's and Florida Subclass Members' Personal Information;

c. failure to disclose that their computer systems and data security practices were inadequate to safeguard Plaintiff Olivieri's and the Florida Subclass' Personal Information from theft.

198. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendants engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Plaintiff Olivieri and the Florida Subclass.

199. In committing the acts alleged above, Defendants engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Plaintiff Olivieri and the Florida Subclass that they did not follow industry best practices for the collection, use, and storage of Personal Information.

200. As a direct and proximate result of Defendants' conduct, Plaintiff Olivieri and the Florida Subclass have been harmed and have suffered damages including, but not limited to increased risk of future identity theft and fraud and time spent monitoring, addressing and correcting the current and future consequences of

the Data Breach.

201. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff Olivieri and the Florida Subclass have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

COUNT XII
Declaratory Relief
(*On Behalf of Plaintiffs and Each Classes Against All Defendants*)

202. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

203. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' duties to safeguard and protect Plaintiffs' and Class Members' Personal Information. Defendants' security measures were (and continue to be) woefully inadequate. Defendants dispute these contentions and contend that their security measures are appropriate.

204. Plaintiffs and Class Members continue to suffer damages and exposure to other injury and harm, and without a declaratory relief, they will likely to continue to suffer further injury, a possibility of a future data breach, and harm.

205. Therefore, Plaintiffs and Class Members request a judicial determination of their rights and duties, and ask the Court to enter a judgment

declaring, *inter alia*, (i) Defendants owed (and continue to owe) a legal duty to safeguard and protect Plaintiffs' and Class Members' confidential and sensitive Personal Information, and timely notify them about the Data Breach, (ii) Defendants breached (and continue to breach) such legal duties by failing to safeguard and protect Plaintiffs' and Class Members' Personal Information, and (iii) Defendants' breach of their legal duties directly and proximately caused the Data Breach, and the resulting damages, injury, or harm suffered by Plaintiffs and Class Members. A declaration from the Court ordering Defendants to stop their illegal practices is required. Plaintiffs and Class Members will otherwise continue to suffer harm as alleged above.

PRAYER FOR RELIEF

1. **Damages.** As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class Members suffered (and will continue to suffer) actual, consequential, incidental, and statutory damages and other injury and harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Personal Information, (iv) statutory damages, (v) deprivation of the value of their Personal Information, for

which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages. Plaintiffs and Class Members also are entitled to equitable relief, including, without limitation, disgorgement and restitution. Plaintiffs' and Class Members' damages were foreseeable by Defendants and exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiffs' and Class Members' claims have been performed and occurred.

2. **Punitive Damages.** Plaintiffs and Class Members also are entitled to punitive damages from Defendants, as punishment and to deter such wrongful conduct in the future. All conditions precedent to Plaintiffs' and Class Members' claims have been performed and occurred.

3. **Injunctive Relief**. Plaintiffs and Class Members also are entitled to injunctive relief in multiple forms including, without limitation, (i) credit monitoring, (ii) Internet monitoring, (iii) identity theft insurance, (iv) prohibiting Defendants from continuing their above-described wrongful conduct, (v) requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the Personal Information entrusted to them, (vi) periodic compliance audits by a third party to ensure that Defendants are properly

safeguarding and protecting the Personal in their possession, custody and control, and (vii) clear and effective notice to Class Members about the serious risks posed by the exposure of the Personal Information and the precise steps that must be taken to protect themselves. All conditions precedent to Plaintiffs' and Class Members' claims for relief have been performed and occurred.

4. **Attorneys' Fees, Litigation Expenses and Costs.** Plaintiffs and Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action**.**

WHEREFORE, Plaintiffs, on behalf of themselves and all members of the Class respectfully request that (i) this action be certified as a class action, (ii) Plaintiffs be designated representative of the Class and (iii) Plaintiffs' counsel be appointed as counsel for the Class. Plaintiffs, on behalf of themselves and members of the Class further request that upon final trial or hearing, judgment be awarded against Defendants for:

(i) actual, incidental, consequential, and nominal damages to be determined by the trier of fact;
(ii) statutory damages;
(iii) punitive damages;
(iv) equitable relief, including restitution, disgorgement of all amounts by which Defendants have been unjustly enriched;
(v) pre- and post-judgment interest at the highest legal rates applicable;

(vi) appropriate injunctive relief;

(vii) attorneys' fees and litigation expenses;

(viii) costs of suit; and

(ix) such other and further relief that the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all issues so triable.

Dated this 15th day of July, 2024.

ROSSBACH LAW, P.C.

By: */s/ William A. Rossbach*
William A. Rossbach

COTCHETT, PITRE & McCARTHY LLP
Thomas E. Loeser (PHV Forthcoming)
Karin B. Swope (PHV Forthcoming)
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Tel: (206) 802-1272
Fax: (650) 697-0577
tloeser@cpmlegal.com.com
kswope@cpmlegal.com

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson, Esq. (PHV Forthcoming)
Yana Hart, Esq. (PHV Forthcoming)
Tiara Avaness, Esq. (PHV Forthcoming)
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
rclarkson@clarksonlawfirm.com
yhart@clarksonlawfirm.com
tavaness@clarksonlawfirm.com

(counsel continued on next page)

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (PHV Forthcoming)
JENNIFER L. MACPHERSON (PHV Forthcoming)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiffs and the Proposed Class